

Review

Theoretical Foundations and Architectural Evolution of Cyberspace Endogenous Security: A Comprehensive Survey

Heming Zhang ^{1,2,*}, Jian Li ², Hong Wang ², Shizhong Xu ¹, Hong Yang ² and Haitao Wu ¹

¹ School of Information and Communication Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu 610041, China; xsz@uestc.edu.cn (S.X.); wuht@cetcs.com (H.W.)

² No. 30 Institute of CETC, Chengdu 610041, China; lij@cetcs.com (J.L.); wangh@cetcs.com (H.W.); yangh@cetcs.com (H.Y.)

* Correspondence: h.m_001@163.com; Tel.: +86-17-308-040-828

Abstract

The endogenous security paradigm has emerged to address the limitations of traditional cybersecurity, which relies on reactive “patching” and struggles against unknown threats, APTs, and supply chain attacks. Centered on the principle that “structure determines security”, it diverges from detection-based approaches by employing systems theory and cybernetics to architect closed-loop systems with “heterogeneous execution, multimodal adjudication, and dynamic scheduling”. This is realized through intrinsic architectural constructs such as dynamism, heterogeneity, and redundancy. Theoretically, it transforms deterministic component-level attacks into probabilistic system-level events, thereby shifting the security foundation from a “cognitive contest” to an “entropy-driven confrontation”. This paper provides a comprehensive review of this paradigm. We begin by elucidating its philosophical foundations and core axioms, focusing on the Dynamic Heterogeneous Redundancy (DHR) model, which converts attacks on specific vulnerabilities into probabilistic events under the core assumption of independent heterogeneous execution entities. Next, we trace the architectural evolution from early mimic defense prototypes to a universal framework, analyzing key developments including expanded heterogeneity dimensions, intelligence-driven dynamic policies, and enhanced adjudication mechanisms. We then explore essential enabling technologies and their integration with cutting-edge trends such as artificial intelligence, 6G, and cloud-native computing. Through case studies of the 5G core network and intelligent connected vehicles, the engineering feasibility of the endogenous security paradigm has been validated, with quantifiable security gains demonstrated. In a live-network pilot of the endogenous security micro-segmentation system for the 5G core, resource consumption (CPU/memory usage) of network function virtual machines remained below 3% under steady-state service loads. The system concurrently maintained microsecond-level forwarding performance and achieved carrier-grade core service availability of 99.999%. These results demonstrate that the endogenous security mechanism delivers high-level structural security with an acceptable performance cost. The paper also critically summarizes current theoretical, engineering, and ecosystem challenges, while outlining future research directions such as “Endogenous Security as a Service” and convergence with quantum-safe technologies.



Academic Editor: Jisu Park

Received: 29 December 2025

Revised: 22 January 2026

Accepted: 6 February 2026

Published: 8 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article

distributed under the terms and

conditions of the [Creative Commons](#)

[Attribution \(CC BY\)](#) license.

Keywords: cyberspace security; endogenous security; dynamic heterogeneous redundancy; mimic defense; security paradigm; network resilience; security architecture

1. Introduction

1.1. Fundamental Challenges to Cyberspace Security

Traditional cybersecurity defense systems are built upon the core assumption of “vulnerability and backdoor awareness”. Their classic paradigms, such as firewalls and intrusion detection systems, essentially form an external threat detection and blocking loop. This paradigm suffers from fundamental structural limitations: it presupposes that defenders can identify, extract, and deploy defenses against vulnerability characteristics, either before or simultaneously with attackers [1]. However, when facing unknown threats (such as zero-day vulnerabilities), the lag in signature databases renders this approach instantly obsolete. When facing Advanced Persistent Threats (APTs), attackers can easily bypass perimeter monitoring based on anomaly thresholds by leveraging legitimate credentials and low-frequency penetration tactics. In supply chain attacks, malicious code is pre-embedded within trusted software and hardware sources, fundamentally undermining all perimeter defenses built on “internal–external distinctions” and “signature verification” [2].

Although advanced detection techniques—such as behavior-based machine learning [3] and threat hunting [4]—aim to identify novel threats through continuous learning, their effectiveness remains contingent upon the recognition and extrapolation of known attack patterns. Consequently, when confronted with truly unknown threats that lie beyond their learned domain, these techniques exhibit inherent limitations. This inherent reliance on prior knowledge ensnares the prevailing security paradigm in a perpetual cycle of reaction, leaving it fundamentally incapable of addressing the root causes of unknown, systemic vulnerabilities.

1.2. The Proposal and Vision of the Endogenous Security Paradigm

To address the fundamental limitations of traditional add-on defense mechanisms against foundational security challenges, a paradigm shift centered on the principle that “structure determines security” has emerged: endogenous security [5]. This shift represents a fundamental reconstruction rooted in system architecture logic, rather than a mere enhancement of existing technologies. Its core tenet holds that security capabilities should be “genes” inherent in system design, not after-the-fact “patches”. The philosophical foundation of this paradigm shift lies in recognizing that the inherent security challenges in cyberspace stem from a fundamental contradiction between the “simplicity” of its universal computing architecture and the “security” it demands. Traditional approaches attempt to patch this contradiction at the application layer, whereas endogenous security advocates for architectural innovation that introduces controlled complexity—such as dynamism, heterogeneity, and redundancy—at the foundational level. The core value of this design lies in its systematic internalization of defense effectiveness as an operational imperative. For instance, dynamism prevents attack surfaces from being statically locked; heterogeneity ensures that no single vulnerability can compromise all execution paths; and redundancy provides fault tolerance against localized failures. Consequently, security is transformed from a “costly add-on” reliant on external awareness into an “inherent property” determined by the system’s internal structure.

The endogenous security paradigm builds its vision around three core objectives [6]:

Dynamic Security: Unlike static, fixed defense configurations, endogenous security employs continuous or triggered self-alteration to make attack surfaces difficult to detect, target, and exploit. This dynamism manifests in resource scheduling, network configurations, execution paths, and algorithmic strategies. It aims to turn attackers’ long-term research advantages against static targets into significant disadvantages in dynamic environments, thereby raising attack costs and uncertainty.

Proactive Security: Traditional defenses operate on a passive “stimulus–response” model. In contrast, endogenous security—through architectural design—endows systems with inherent, spontaneous threat suppression and proactive defense capabilities. For example, systems based on Dynamic Heterogeneous Redundancy (DHR) employ adjudication mechanisms that compare output discrepancies across heterogeneous execution entities in real time. This enables autonomous detection and isolation of anomalies without relying on attack signature databases, achieving a self-contained “detect–mitigate” loop against unknown threats [7]. This marks a shift from “identifying known malicious behavior” to “validating unknown anomalies”.

Quantifiable Security: This objective represents a critical step for endogenous security to advance from empirical approaches toward engineering science. While traditional security struggles to answer “Is it sufficiently secure?”, inherent security seeks to quantify security gains, reliability, and availability within specific architectures through mathematical modeling (e.g., probability-based reliability models) and experimental validation. For instance, given fixed heterogeneity and dynamic policies, it can theoretically calculate the lower-bound probability of a system successfully resisting specific attack types, providing objective, measurable grounds for security design and assessment.

To realize this vision, research in endogenous security is advancing along two core trajectories: theoretical deepening and architectural evolution. Theoretically, the field has progressed from early models such as Dynamic Heterogeneous Redundancy (DHR) and Mimetic Defense principles toward more formalized security theorem proofs and universally applicable security construction theories. Architecturally, it has evolved from dedicated hardware prototypes into software-defined, virtualized, and service-oriented universal security architectures tailored to complex scenarios such as cloud computing, edge computing, 5G/6G core networks, and the industrial Internet. Deep integration with technologies like artificial intelligence and trusted computing continues to broaden its application boundaries.

This paper adopts a clear dual-track narrative: First, it traces the theoretical development trajectory, systematically elucidating the conceptual origins of endogenous security, its core axioms, formal models, and mathematical interpretations of security mechanisms—revealing how it overcomes the limitations of traditional defense. Second, it examines the architectural evolution, tracing the path from proof-of-concept systems to standardized reference designs and further to integration with emerging computing environments, while analyzing engineering challenges and solutions.

The primary contributions of this paper are:

1. First, through a systematic analysis that treats the theoretical development and architectural evolution of endogenous security as two parallel and synergistic threads, this review delineates a comprehensive panorama of its technological maturation.
2. Second, it deeply dissects the latest dynamics and potential directions for integrating endogenous security with cutting-edge trends such as artificial intelligence, cloud-native technologies, and future networks.
3. Third, it critically summarizes current theoretical and engineering challenges while proposing several open questions to guide future research.

This review aims to provide a comprehensive reference for academia and industry on the current state and future trends of the endogenous security paradigm, fostering deeper and broader advancements in the field.

1.3. Review Methodology

This review employs a systematic literature review methodology to ensure transparency, rigor, and reproducibility. The aim is to comprehensively trace the theoretical

and architectural evolution of “endogenous security in cyberspace” from its conceptual inception in January 2013 to October 2025. Literature searches were conducted across core Chinese and English academic databases, including Web of Science, IEEE Xplore, ACM Digital Library, and CNKI. Keyword combinations—such as “endogenous security”, “cyberspace mimic defense” and “dynamic heterogeneous redundancy”—were used for retrieval and citation tracking.

The search initially identified 852 relevant documents. Screening was performed in two stages:

1. **Title/Abstract Screening:** Documents that were clearly irrelevant, non-academic (e.g., news reports, commercial promotions), or in languages other than Chinese or English were excluded, yielding 213 papers.
2. **Full-Text Screening:** After obtaining and reviewing the full texts, papers were further excluded if they (a) did not focus on endogenous security or its core models, (b) lacked clear methodological descriptions, (c) had inaccessible full texts, or (d) were deemed low in academic quality.

Finally, 85 high-quality papers were included for in-depth analysis.

Literature screening was conducted based on the following criteria. Inclusion criteria encompassed high-quality academic works primarily focused on endogenous security or its core models (e.g., DHR, mimic defense), covering theory, architecture, evaluation, or applications. Exclusion criteria included publications that only peripherally mentioned the topic or lacked substantive empirical or theoretical contributions. From the final corpus, information on research themes, core contributions, technical solutions, evaluation methods, and conclusions was systematically extracted. Guided by the dual analytical threads of “theoretical development” and “architectural evolution”, thematic analysis was employed to synthesize the findings and critically discuss key milestones, challenges, and trends within the paradigm.

2. The Theoretical Foundations of Endogenous Security

2.1. Philosophical Thought and Core Definitions

The philosophical foundation of the endogenous security paradigm stems from a fundamental epistemological shift in understanding the intrinsic contradictions of cyberspace. It is anchored in two core tenets: the “unity of opposites between functionality and side effects” and the notion that “intrinsic contradictions drive development”.

Traditionally, security vulnerabilities have been viewed as “defects” or “errors” in system functionality, to be eliminated through external patches [8]. In contrast, endogenous security re-conceptualizes the issue from a fundamentally different perspective. Analogous to pharmaceuticals that deliver therapeutic benefits alongside inevitable side effects, the von Neumann-based universal computing architecture—despite providing unparalleled flexibility and openness—inherently generates vulnerabilities and backdoors as “side effects”, stemming from its simple, deterministic, and open nature. In this analogy, the “chemical certainty” of a drug corresponds to the “execution certainty” of system logic; its “targeted action” corresponds to “intended functionality”; and its inevitable “side effects” correspond to the emergent “unintended attack surface”. Thus, functionality and these security deficits exist in a symbiotic yet contradictory relationship.

Consequently, the solution to security challenges lies not in pursuing the illusion of “absolute security” without side effects. Instead, it requires innovative architectural design to proactively harness this contradiction, rendering the side effects controllable, utilizable, or even transforming them into security assets. This constructive engagement is the essence of the “unity of opposites”. The advancement of security is thus driven by recognizing

and leveraging this inherent structural tension, rather than merely reacting to external threats—hence, “development driven by internal contradictions”.

Building on this philosophy, endogenous security can be defined as: a systemic attribute whereby a system’s inherent structural design (e.g., dynamic, heterogeneous, redundant) enables it to autonomously generate security capabilities from its own architecture, thereby effectively countering uncertain threats such as unknown vulnerabilities and backdoors [9]. It emphasizes the “generative potential” and “intrinsic origin” of security.

This core definition clarifies its relationship with adjacent concepts like “resilience” and “trusted computing”, highlighting both connections and fundamental distinctions:

Connection vs. Distinction with “Resilience”: Both aim to ensure a system’s sustained operation under threat. The key distinction lies in their focus: resilience concerns a system’s ability to resist, recover, and adapt after damage occurs, representing a consequence-oriented robustness. Endogenous security, conversely, focuses on making attacks inherently difficult to succeed from the outset through intrinsic construction, embodying a preemptive immunity. Thus, an endogenous security architecture provides a more robust foundation for resilience.

Connection vs. Distinction with “Trusted Computing”: Both emphasize building trust from the ground up. The fundamental difference lies in the trust model: Trusted computing relies on hardware-based “roots of trust” and builds a static, incremental chain of trust through measurement, with its core being the verification of known, expected states. Endogenous security, however, does not assume or rely on fixed trusted components. Through constructs like dynamic heterogeneous redundancy, it achieves overall security by architecturally tolerating the failure or compromise of unknown, untrusted components, using mechanisms like diverse execution and adjudication. The two paradigms are complementary: trusted computing can provide a purer initial environment for endogenous security’s execution entities, thereby strengthening its operational foundation [10].

As summarized in Table 1, endogenous security distinguishes itself from contemporary paradigms through its foundational philosophy of Security by Construction. Unlike MTD which perturbs the attack surface or Zero Trust which controls access, endogenous security aims to architecturally invalidate the exploitability of vulnerabilities. This comparison clarifies its complementary role: while ZTA secures the access path and Resilience ensures operational continuity, endogenous security targets the intrinsic robustness of the system core itself, offering a distinct layer of defense against unknown threats.

Table 1. Comparison of Endogenous Security with Other Mainstream Security Paradigms.

Dimension	Endogenous Security	Moving Target Defense	Resilience	Zero Trust	Trusted Computing
Core Philosophy	Security by Construction: Embeds security as an inherent property via architectural dynamics, heterogeneity, and redundancy.	Dynamic Randomization: Increases attack cost/uncertainty by persistently altering system attributes [11].	Survive & Recover: Ensures continuity of core functions and rapid recovery post-compromise.	Never Trust, Always Verify: Eliminates implicit trust; mandates continuous authentication and least-privilege access.	Hardware Root of Trust: Establishes and extends trust from a hardware root via verified measurements.
Security Paradigm	Proactive Construction: Prevents attack success through inherent architectural design.	Proactive Perturbation: Perturbs the attack chain by adding a layer of dynamism.	Reactive Adaptation: Focuses on post-disruption resistance, recovery, and adaptation.	Continuous Verification: Dynamically assesses risk and grants minimal necessary access.	State Verification: Verifies system/components conform to a known, trusted baseline.

Table 1. Cont.

Dimension	Endogenous Security	Moving Target Defense	Resilience	Zero Trust	Trusted Computing
Trust Model	Dynamic Relative Trust: Achieves overall trust via multi-execution & adjudication, without presuming component trustworthiness.	Trust-Neutral: Effectiveness relies on change strategies, not on altering intrinsic trust.	Post-Trust Survival: Concerned with system survivability after trust is broken.	Dynamic Minimal Trust: Defaults to distrust; grants trust dynamically based on continuous risk assessment.	Static Transitive Trust: Trust propagates statically from a hardware root up through a measurement chain.
Primary Focus	Architectural immunity to unknown vulnerabilities/backdoors.	Increasing cost of attacks reliant on staticity/predictability.	Service continuity and business recovery from disruptions.	Access control to prevent lateral movement/unauthorized access.	System/software integrity against tampering and malware.
Key Limitation	Engineering challenges: formal proof, resource management, adjudicator protection.	Limited against insider threats; potential performance overhead; strategies may be learned.	Does not inherently reduce attack success probability.	Operational complexity and dependency on identity management.	Hardware dependency; cannot address hardware-level backdoors.

2.2. Core Security Axioms and Assumptions

Traditional security systems are grounded in a “cognitive a priori assumption”: that defenders can progressively approach comprehensive threat awareness through the continuous accumulation of knowledge (e.g., signature databases, behavioral models, threat intelligence). This premise places defense in a sustained “cognitive race”, wherein defenders operate from a position of perpetual latency, fundamentally limiting the paradigm’s capacity to address unknown threats.

It should be acknowledged that contemporary hybrid defense approaches—such as behavior-based detection and proactive threat hunting [4]—have sought to mitigate this limitation by relaxing the strict a priori requirement. By employing techniques such as continuous learning to model system or user behavior, they enhance the detection of novel attack patterns. However, their effectiveness remains contingent upon the cognitive recognition of such patterns, whether predefined or learned inductively. Thus, while these methods represent a significant advance, they do not transcend the core structural constraint of the cognitive paradigm: the inherent inability to counter truly unknown threats that fall outside the system’s learned or inductive scope.

In contrast, endogenous security is founded on a distinct set of constructive axioms independent of prior knowledge [12]. Its theoretical core consists of three fundamental axioms: the Axiom of Heterogeneity, the Axiom of Transformation, and the Axiom of Redundancy. These principles are designated as axioms because they jointly constitute the logical and formal bedrock of the paradigm. Their validity is assumed as intrinsic within this framework, thereby providing the foundation for deriving specific security models, quantifying defensive benefits, and guiding the design of system architectures.

1. **Axiom of Heterogeneity:** Security can be enhanced by constructing multiple, functionally equivalent execution entities that are heterogeneously implemented (differing in hardware, software, algorithms, or parameters). This axiom recognizes that attack success is often tightly coupled with specific implementation details. Heterogeneity ensures that a single vulnerability cannot simultaneously compromise all execution paths, thereby transforming attack “certainty” into “probability”.

2. **Axiom of Transformation:** Security is positively correlated with dynamic transformations over time, such as changes in resource allocation, network topology, or execution policy. This axiom acknowledges that static targets afford attackers prolonged windows for reconnaissance, validation, and exploitation. Continuous or triggered transformations render the attack surface non-stationary, turning the system from a “fixed target” (easy to detect and attack) into a “moving target” (hard to detect and attack).
3. **Axiom of Redundancy:** By constructing resource and functional redundancy alongside collaborative, multi-modal arbitration mechanisms, a system can internally detect, isolate, or tolerate failures or anomalies within a defined subset of its components (which may be under attack). This axiom grants the system inherent “intrusion tolerance” and “self-healing” capabilities.

These three axioms do not operate in isolation. Their most profound strength emerges from their synergistic interaction, which generates systemic security gains. Dynamic Transformation injects unpredictability into heterogeneous redundancy, preventing attackers from reverse-engineering components over time. In turn, heterogeneous redundancy provides diverse primitives for transformation and a fault-tolerant foundation. Together, they form a closed-loop “construction-sensing-feedback” system, whose security derives from the intrinsic “uncertainty” imposed on attackers through spatio-temporal structural superposition.

The axiomatic framework of endogenous security represents a fundamental paradigm shift. It moves away from a reliance on identifying “known malicious entities” and instead focuses on designing architectures that confer inherent, quantifiable “immunity” and “resilience”. Its efficacy depends not on recognizing threats, but on structurally disrupting, diluting, and tolerating their effects [13].

2.3. Key Model

2.3.1. Formal Description of Dynamic Heterogeneous Redundancy Models

The Dynamic Heterogeneous Redundancy (DHR) model [14] provides both the core engineering implementation and the formal foundation for the endogenous security concept. Functionally, it operates as a closed-loop negative-feedback control system with integrated “perception-decision-scheduling” capabilities, achieving deterministic security through engineered structural uncertainty.

The model can be formally defined as an abstract system comprising three core components:

- **Heterogeneous Execution Pool:** A set of multiple, functionally equivalent execution entities that are heterogeneous in their implementation (e.g., hardware, OS, algorithms, or parameters). These entities process identical input tasks in parallel, each producing an independent output. This heterogeneity is the security cornerstone, ensuring that the same exploit manifests as distinct vulnerabilities across different entities.
- **Multi-mode Arbiter:** Acting as the system’s “security brain”, the arbiter receives and compares all executor outputs in real time. Its core function is to determine and output a trusted result from potentially inconsistent outputs based on a predefined strategy (e.g., majority voting, threshold judgment), while simultaneously identifying and flagging anomalous executors.
- **Feedback Controller & Scheduler:** Driven by anomaly signals from the arbiter, this component dynamically manages the system state. Its key actions include sanitizing, resetting, or repairing flagged executors, and dynamically scheduling, replacing, or reorganizing entities within the pool. This continuous adjustment alters the system’s attack surface over time.

Together, these components form an autonomous “perception-adjudication-scheduling” closed loop. The security gain of the DHR model stems not from identifying specific attacks, but from the spatial fault tolerance inherent in its heterogeneous redundancy [15] and the temporal uncertainty introduced by its dynamic scheduling. Their synergy ensures that attacks targeting component-level vulnerabilities cannot be reliably sustained at the system level. Consequently, security is transformed from a passive attribute reliant on external alerts into an active capability generated by the intrinsic architecture itself [16].

2.3.2. Analysis of Safety Enhancement Mechanisms

The security efficacy of the DHR model arises from its architectural design, which systematically transforms an attacker’s advantage in exploiting specific vulnerabilities into probabilistic uncertainty regarding attack success [17].

This transformation is achieved through a triple-synergy mechanism:

- **Spatial Defense via Heterogeneous Redundancy:** This forms the first defensive layer. Because multiple, functionally equivalent execution entities operate in parallel with inherent implementation heterogeneity, an attack payload targeting a specific vulnerability in one entity cannot produce identical effects on others. This prevents a single-point exploit from simultaneously compromising all output paths, thereby confining attacks to localized components.
- **Temporal Uncertainty via Dynamic Scheduling:** The feedback control loop continuously or selectively alters the active set of executors and their configurations. Consequently, even if an attacker successfully exploits a vulnerability in a specific executor at time t^* , their attack vector may rapidly become ineffective as the target is scheduled offline or its environment changes. This drastically compresses the viable attack window, disrupting the continuous cycle of reconnaissance, exploitation, and lateral movement.
- **Anomaly Neutralization via Multi-mode Adjudication:** The arbiter performs real-time comparison of outputs from all heterogeneous executors. Any anomalous output from a compromised executor is identified and discarded due to its inconsistency with the majority. The system’s correct output is thus guaranteed by consensus or more sophisticated strategies, ensuring that the failure of one or several components does not lead to system failure.

The security of the Dynamic Heterogeneous Redundancy (DHR) model is predicated on the statistically independent failure of its heterogeneous executors. This core assumption can be contested in real-world settings by common-mode attacks that target vulnerabilities common to multiple executors, such as those originating from shared design logic or a homogeneous supply chain. Essentially, DHR’s strategy transcends the conventional goals of attack prevention or detection. Instead, it employs architectural means to transform a deterministic component-level exploit into a system-level event of quantifiably low probability. This attack success probability can be formally modeled, and is governed by parameters like the heterogeneity degree, executor pool size, and dynamic scheduling policy. Therefore, DHR represents a paradigmatic transition: from security dependent on threat recognition to one grounded in the probabilistic convergence guaranteed by structural resilience.

2.4. Threat Model and Adversarial Assumptions

This section articulates the threat model and core adversarial assumptions underlying the Dynamic Heterogeneous Redundancy architecture. By defining the security boundaries and evaluation premises, it formally establishes the conditions under which DHR’s key security proposition—the conversion of deterministic attacks into probabilistic events—is substantiated.

2.4.1. Assumed Capabilities and Knowledge of the Adversary

This model posits that the adversary (A) possesses the following capabilities and knowledge:

- **Full Exploitation Capability:** The adversary can exploit unknown vulnerabilities (e.g., 0-day), design backdoors, or configuration errors to fully compromise and control one or more execution entities. This enables data theft and the tampering of internal logic or outputs.
- **Limited Prior Knowledge:** Initially, the adversary lacks complete vulnerability information for all heterogeneous execution entities and is unaware of the system's real-time dynamic scheduling policies. Acquiring this intelligence requires continuous reconnaissance.
- **Non-Instantaneous Coordination:** Compromising different heterogeneous entities is a sequential process requiring time for reconnaissance, adaptation, and attack. DHR's dynamic design aims to disrupt and compress this timeline, thereby increasing the difficulty of mounting a coordinated attack across all entities.
- **Inability to Subvert Cryptographic Foundations:** The adversary cannot break the cryptographic primitives (e.g., secure hash functions, digital signatures) used to ensure secure communication between entities, identity authentication, and code integrity verification.

2.4.2. System Trust Boundaries and Security Assumptions

The efficacy of the DHR architecture is predicated on the following critical trust assumptions:

- **Trustworthiness of the Arbiter and Scheduler:** The multi-modal arbiter and the feedback-controlled scheduler constitute the Trusted Computing Base of the system. They must be implemented within a hardware-protected trusted execution environment or as formally verified, high-assurance modules. This assumption is fundamental; a compromised arbiter would lead to a catastrophic failure of the security mechanism.
- **Initial Cleanliness of the Resource Pool:** During system initialization or reconfiguration, the execution entity instances drawn from the heterogeneous resource pool are assumed to be free of pre-embedded, targeted malicious code. The system relies on dynamic reset, sanitization, and scheduling to mitigate runtime contamination.
- **Reliable Functional Equivalence:** All heterogeneous execution entities, when processing valid inputs, must produce semantically consistent outputs that conform to the prescribed specifications. This reliability is essential for the effective operation of the multi-modal adjudication mechanism.

2.4.3. Core Defense Focus and Applicable Scenarios

Based on the aforementioned assumptions, the DHR architecture is primarily designed to counter the following two attack scenarios:

- **Attacks Leveraging Specific Vulnerabilities:** This is the primary defense target. The architectural heterogeneity ensures that a single vulnerability cannot compromise all execution paths, while its dynamism causes the reconnaissance and exploit cycle against a specific target to become obsolete quickly.
- **Non-Coordinated, Incremental Penetration:** An attacker attempting to probe and compromise entities sequentially to gain majority control is mitigated by DHR's adjudication mechanism, which isolates anomalous outputs from a minority of compromised entities. Concurrently, dynamic scheduling replaces suspected or confirmed compromised units, thereby resetting the attacker's foothold.

3. The Evolutionary Path of the Endogenous Security Architecture

3.1. Early Architecture: Prototypes and Practices of Mimetic Defense

The evolution of endogenous security architecture began with the engineering realization of its core theory, Dynamic Heterogeneous Redundancy (DHR). Early prototypes, such as mimic routers and firewalls, served as proof-of-concept implementations [18]. These systems integrated multiple functionally equivalent yet heterogeneously implemented executors. A centralized multi-modal adjudicator compared their outputs, and a negative-feedback controller dynamically managed anomalous executors, thereby forming a closed-loop defense system.

These early efforts validated the feasibility of constructing an “uncertain environment” to proactively defend against unknown vulnerabilities and backdoors. Their security efficacy was empirically substantiated through high-profile live-fire exercises, such as the “Qiangwang” International Mimic Defense Challenge. For example, in a 2020 test, mimic-based industrial internet devices withstood over 950,000 high-intensity attacks from 40 teams across several days without service disruption [19]. Furthermore, benchmark tests (e.g., “Mimic Construction Benchmark Testing”) mechanistically verified quantifiable metrics, including a near-100% suppression rate against differential-mode disturbances [20].

However, this architectural phase had significant limitations. First, its defense is strictly bounded by a predefined “mimic defense boundary”—the system’s specified I/O and security perimeter. This is an inherent constraint of the DHR model: its adjudication-based mechanism ensures security only within this boundary, leaving it vulnerable to out-of-bound attacks (e.g., social engineering). Second, early prototypes were largely dedicated hardware or custom systems with relatively static strategies for resource heterogeneity and scheduling, struggling to balance overhead, complexity, and generality [21]. Consequently, their deployment in dynamic, cloud-virtualized environments was limited. Notably, while the first limitation is intrinsic to the model, the second became a key driver for the architecture’s evolution toward generalized, software-defined paradigms.

3.2. Evolution and Expansion: From Concept to Universal Framework

3.2.1. Extension of the Dimension of Heterogeneity

The evolution of endogenous security architectures has been propelled by the deepening understanding and implementation of “heterogeneity” as a foundational element [22]. This has enabled a significant expansion from single-dimensional, static approaches to multi-dimensional, dynamic ones.

Early prototypes relied chiefly on physical-layer heterogeneity (e.g., hardware from different vendors or distinct OS kernels). While effective against vulnerabilities in specific hardware/software chains, this approach incurred high resource costs and offered limited flexibility. To build more efficient and universally applicable systems, the dimensions of heterogeneity have been systematically broadened across three key layers:

1. **Algorithmic and Implementation Heterogeneity:** Under identical functional specifications, systems employ multiple algorithms based on distinct principles, each with independently developed code. For example, image encoding might concurrently use encoders for different standards (e.g., JPEG, WebP), while cryptographic operations run implementations from separate libraries (e.g., OpenSSL, BoringSSL) [23]. This compels attackers to exploit entirely independent vulnerabilities across disparate codebases, drastically increasing the attack complexity.
2. **Parameter and Configuration Heterogeneity:** On identical hardware and software bases, systems introduce uncertainty at the micro-execution level by dynamically adjusting critical runtime parameters—such as randomized memory layouts, compiler optimization flags, or task scheduling policies. This “lightweight” heterogeneity

strategy significantly reduces resource overhead while effectively disrupting attacks that depend on predictable memory states or execution timing.

3. Virtual and Cloud Resource Heterogeneity [24]: With the advent of mainstream cloud computing, heterogeneity has been abstracted into the differentiated orchestration of virtualized resource pools. Systems can dynamically assemble service instances from diverse physical hosts, virtualization technologies (KVM 5.10, Xen 4.15), container runtimes (Docker 20.10+, Kata Containers 2.4), or geographic regions to create logically unified yet physically distributed, dynamic execution environments. This not only preserves the benefits of hardware diversity but also enables elastic provisioning and automated orchestration [25].

This dimensional expansion of heterogeneity—from physical fixity to logical variability, from coarse-grained to fine-grained, and from entity-bound to policy-defined—marks a pivotal evolution for endogenous security. The paradigm has transformed from a hardening technique for specialized devices into a universal security construction method that can be flexibly embedded within modern, complex, elastic, and service-oriented IT architectures. Consequently, security gains now transcend the constraints of costly physical diversity. Instead, they are efficiently generated and delivered on-demand across vast virtualized infrastructures through software-defined, intelligently orchestrated means.

3.2.2. Intelligent Dynamic Strategy

The evolution of dynamic policies within endogenous security architectures marks a profound transition: from simply “introducing uncertainty” to actively “pursuing intelligent optimization”.

Early systems primarily relied on random or round-robin scheduling, with the core aim of disrupting attackers’ static assumptions by adding temporal unpredictability, thereby increasing attack difficulty. While effective, this indiscriminate dynamism was essentially “blind action”, potentially incurring unnecessary performance overhead without offering optimal, context-aware responses to specific threats.

Advances in artificial intelligence are propelling dynamic strategies toward intelligent, perception-driven approaches [26]. The core of this shift is the establishment of a feedback control loop that integrates real-time security posture, resource state, and performance metrics, enabling three key intelligent scheduling modes:

1. Threat-Aware Scheduling: The system continuously monitors the threat landscape via external intelligence, internal anomaly detection (e.g., adjudicator inconsistency rates), or active probes. Scheduling policies then adapt dynamically—for instance, increasing transformation frequency during sustained scanning to compress attack windows, or proactively isolating and re-diversifying resource pools upon detecting anomalies targeting specific component types, enabling precise, threat-informed defense.
2. Performance-Load-Aware Scheduling: Scheduling decisions holistically consider Quality of Service (QoS) metrics such as system resource utilization and service latency. The objective is to dynamically balance security and efficiency. For example, more aggressive, resource-intensive scheduling may be employed during off-peak hours to elevate security levels [27], while conservative strategies that prioritize core service performance are activated during peak loads.
3. Adaptive Scheduling via Reinforcement Learning (RL): This represents the frontier of intelligent dynamism. Through continuous interaction with its environment (encompassing both attack patterns and workload states), the system uses RL algorithms to autonomously learn and converge on optimal scheduling policies (e.g., timing, target selection) for specific contexts [28]. This approach aims to achieve long-term global optimization by maximizing security gains while minimizing performance costs.

However, the deep integration of artificial intelligence (AI)—particularly reinforcement learning (RL)—into the endogenous security scheduling loop introduces novel challenges and risks, defining a key frontier for research. A primary concern is the robustness of the RL agents themselves: they are susceptible to adversarial attacks that can mislead or poison their decision models, while the training process often faces instability and convergence issues in complex, dynamic environments, compromising policy reliability. Importantly, the endogenous security architecture itself provides a unique foundation to mitigate these risks. Its inherent dynamic heterogeneous redundancy (DHR) and multimodal adjudication mechanisms can architecturally detect and tolerate anomalies in individual intelligent schedulers' outputs. This creates a natural sandbox and fault-tolerant framework for the secure training, validation, and deployment of these advanced “intelligent immune” components.

This intelligent evolution signifies that endogenous security is advancing from a passive defense reliant on “structural randomness” to an active, environment-aware system capable of autonomous decision-making and dynamic strategic interaction. The system thus transforms from a mere executor of fixed rules into an adaptive organism that intelligently allocates its intrinsic defensive resources based on real-time conditions, achieving optimal security efficacy [29].

3.2.3. The Evolution of the Adjudication Mechanism

The evolution of arbitration mechanisms in endogenous security architectures marks a critical capability leap: from rudimentary judgments based on “quantitative consistency” to intelligent diagnostics capable of discerning “deep behavioral anomalies”.

Early DHR systems predominantly employed simple majority voting (or fixed-threshold arbitration). The logic was straightforward: when most heterogeneous executors produced consistent outputs, the result was deemed correct, while minority inconsistencies were flagged as anomalies [30]. However, this mechanism has inherent limitations [31]:

1. It implicitly assumes compromised executors remain in the minority, potentially failing against sophisticated attacks that simultaneously affect multiple entities (e.g., via common design flaws).
2. Its applicability is restricted to discrete, deterministic output comparisons. It struggles with legitimate but manipulated outputs (e.g., from implanted backdoors) or with complex, continuous outputs like images or text.

Driven by advances in machine learning, arbitration is now evolving toward deep behavioral anomaly diagnosis. The core innovation is that the adjudicator no longer merely compares the “superficial consistency” of final outputs. Instead, it continuously monitors and analyzes the multi-dimensional runtime behavior of each executor—including system call sequences, resource consumption patterns, memory access traces, computational intermediate states, and even microsecond-level execution timing deviations. This enables the construction and continuous updating of a dynamic “normal behavior baseline” model per executor or task category.

Consequently, when an attack occurs, even if malicious code crafts a superficially normal final output, subtle execution anomalies—such as initiating covert network connections or accessing anomalous memory regions—become exceedingly difficult to conceal from the behavioral analysis model. However, this advanced adjudication mechanism based on deep behavioral analysis entails significant practical deployment challenges, primarily concerning privacy, data volume, and real-time performance. First, fine-grained runtime monitoring raises privacy and compliance concerns, necessitating safeguards such as data anonymization and the use of Trusted Execution Environments (TEEs) for processing sensitive information. Second, building accurate behavioral models depends on massive training datasets, imposing significant demands on data infrastructure and motivating

research into lightweight models and incremental learning. Finally, meeting the low-latency requirements of mission-critical systems while maintaining high adjudication accuracy is a core engineering hurdle, necessitating optimal trade-offs between model complexity, feature selection, and inference speed. Progress in addressing these challenges constitutes an active research frontier and will directly determine the depth and breadth of integration for behavioral adjudication within endogenous security architectures.

This evolution expands the scope of security arbitration from a singular “output space” to a rich “behavioral space” [32], significantly enhancing detection of unknown attacks and stealthy backdoors while reducing reliance on absolute numerical superiority among executors. It endows the architecture with a more profound “immune system” characteristic: the ability not only to identify obvious “foreign invaders” but also to sense subtle “pathological” shifts in the internal behavioral patterns of its own components, enabling earlier and more precise warning and isolation.

Although this intelligent approach introduces new challenges—such as the need for training data, feature engineering complexity, and false positive control—it unequivocally marks the evolution of endogenous security arbitration toward deep, context-aware perception.

3.3. Standardization and Reference Architecture

A hallmark of endogenous security’s maturation from foundational theory to industrial practice is the systematic formulation and refinement of reference architectures and technical standards. This standardization endeavor, which has evolved from domestic and industry-led initiatives to gain international recognition, is tightly coupled with concrete industrial applications, thereby providing the essential framework for scalable and replicable technological deployment. To illustrate the significant progress achieved across this multilayered standards landscape, representative examples are presented in Table 2 to chart its evolution, which is not an exhaustive list.

Table 2. Overview of Representative Standards for Endogenous Security.

Standard Tier	Representative Standard	Lead/Drafting Organization(s)	Core Content & Significance	Deployment Status
Domestic Consortium Standards	T/ZGTXXH 043—2022 Intrinsic Security Architecture for Network 5.0 [33]	China Communications Standards Association	Defines terminology, overall architecture, and an authentication and trust transfer mechanism based on trusted identifiers for endogenous security networks, providing a top-level design framework for future network architectures.	Conceptual/ Framework
Domestic Consortium/Industry Standards	T/NJCESS 003-2024 Technical Specification for Intrinsic Security Network Controllers [34]	Purple Mountain Laboratory, et al.	Specifies endogenous security capability requirements for network controllers, including heterogeneous redundant executor groups, providing criteria for the security design and evaluation of cloud-network infrastructure controllers [35].	Pilot/Validation
International Standard	GSMA FS.61 5G Core Network Resource Pool Micro-segmentation Guidelines [36]	China Mobile, etc. (promoted within GSMA)	The first international standard for a specific technology under the “endogenous security” paradigm, promoting the original micro-segmentation scheme to global mobile communication systems [37].	Large-scale Commercial Deployment (Promotion Ongoing)

Table 2. *Cont.*

Standard Tier	Representative Standard	Lead/Drafting Organization(s)	Core Content & Significance	Deployment Status
Domestic Industry Standards	YD/T 6021-2024 Technical Requirements for Micro-Segmentation Systems in Cloud-Based Telecommunication Networks [38]	CCSA (China Communications Standards Association)	Details the general framework and functional requirements for micro-segmentation systems, laying the direct technical foundation for implementing endogenous security in scenarios like 5G core networks [39].	Large-scale Commercial Deployment

Taking China Mobile's 5G core network endogenous security micro-segmentation solution as a case in point, it has not only established an industry standard within the China Communications Standards Association (CCSA) but has also achieved international standardization with GSMA FS.61 [36] through the global mobile communications organization GSMA. This milestone represents the first international recognition of China's pioneering endogenous security concepts and engineering practices, offering a "Chinese solution" for global 5G and future network security.

Standardization has served as a direct catalyst, propelling the technology from the laboratory to large-scale industrial application and charting a clear development trajectory:

1. **Architecture and Equipment Standardization:** From the top-level design of the "Network 5.0 Endogenous security Architecture" to specifications for over 40 types of equipment—including network controllers and mimic routers/firewalls—a standardized technical system encompassing "architecture, equipment, and interfaces" has been established.
2. **International Standardization in Critical Scenarios:** In the cutting-edge field of intelligent connected vehicles, an innovation consortium led by the Purple Mountain Laboratories successfully initiated the world's first international standard for endogenous security in vehicle-to-everything (V2X) networks, paving the way for secure and trustworthy autonomous driving.
3. **Large-Scale Commercial Deployment:** The establishment of standards has facilitated extensive commercial rollout. Examples include: intrinsically secure 5G small cells deployed for demonstration across 28 provinces; the endogenous security micro-segmentation system scheduled for nationwide deployment in 5G core networks by 2025, covering approximately 200,000 network element virtual machines; and intrinsically secure MCU chips already applied in critical power infrastructure such as substation monitoring systems [37–40].

The standardization journey of endogenous security has evolved from early theoretical prototypes and consortium standard explorations into a comprehensive, multi-dimensional standards system. This system now covers overall architecture, critical equipment, and scenario-specific technologies, achieving a significant leap from domestic industry standards to international adoption. This process not only signifies technological maturity but also forms the essential foundation for integrating and empowering the endogenous security paradigm within critical information infrastructure—such as 5G, V2X networks, and energy systems—thereby enabling the growth of a robust industrial ecosystem.

4. Enabling Technologies and Cutting-Edge Integration

4.1. Foundational Enabling Technologies

The transformation of the endogenous security architecture from theoretical model to engineering practice—realizing its core “dynamic, heterogeneous, redundant” constructs—relies on a suite of mature foundational technologies. While not exclusive to endogenous security, their characteristics align perfectly with its requirements, forming the essential technological bridge that converts security concepts into system attributes.

First, virtualization and containerization serve as the logical foundation for building efficient, elastic, and redundant resources. By abstracting and pooling computing, storage, and network assets, these technologies enable the on-demand, rapid creation, destruction, or migration of numerous functionally equivalent yet isolated execution entity instances [41]. This directly addresses the high cost and inflexibility of early hardware-based heterogeneous solutions, enabling the flexible orchestration and reconfiguration of heterogeneous resource pools with minimal overhead in seconds or even milliseconds.

Second, Software-Defined Networking (SDN) provides critical control-plane capabilities for establishing dynamic, governable connectivity between execution entities. By decoupling control logic from data forwarding, SDN allows centralized controllers to programmatically adjust network topologies, access paths, and traffic policies in real time based on security directives [42]. This extends “dynamism” beyond computational resource replacement to the network connectivity layer. It facilitates the proactive isolation of anomalous entities or the reconfiguration of communication links, significantly raising the bar for attackers attempting to maintain persistent connections or execute lateral movement.

Finally, Trusted Execution Environments (TEEs) furnish hardware-level trust anchors, strengthening the Root of Trust for individual execution entities. Leveraging processor-based, hardware-isolated secure enclaves, TEEs guarantee the confidentiality and integrity of critical code and data even if the host operating system is compromised. Executing vital security logic or sensitive tasks within a TEE effectively prevents the underlying tampering of the execution entity itself, thereby enhancing the reliability of multi-mode arbitration and the overall robustness of the endogenous security architecture [43].

In summary, virtualization/containerization, SDN, and TEEs provide indispensable implementation methods for the endogenous security architecture at the resource, network, and trust foundation levels, respectively. They transform the system’s inherent “dynamic”, “heterogeneous”, and “redundant” traits from design principles into quantifiable, deployable, and autonomously maintainable technological realities, powerfully propelling the paradigm from academic prototype to industrialized, universal solution.

4.2. Integration and Evolution with Cutting-Edge Technologies

4.2.1. The Empowerment of Artificial Intelligence

The integration of the endogenous security architecture with artificial intelligence marks its evolution from reliance on “engineered structural uncertainty” to a new stage defined by “autonomous evolution and intelligent game-playing”, aiming for dynamic, self-sustaining adaptive capabilities. AI does not replace the core of endogenous security but acts as a pivotal intelligent enhancement, deeply embedded within its closed-loop perception-decision-optimization system to elevate adaptability and proactive defense [44].

Specifically, AI empowerment manifests across three primary dimensions:

1. **Intelligent Anomaly Detection:** Moving beyond traditional arbitration based on output comparison or fixed rules, AI—particularly deep learning models—can analyze massive, multi-dimensional runtime data (e.g., system call sequences, resource fingerprints, micro-features of network traffic) to construct more precise “normal behavior baselines”. This enables the detection of covert, low-frequency, or novel anomalies

that elude conventional methods. Furthermore, using technologies like graph neural networks, AI can trace anomaly propagation across multiple execution entities, facilitating rapid attack localization and root-cause analysis.

2. **Attack Intent Prediction:** Transcending reactive responses to isolated events, AI correlates external threat intelligence with internal system logs. By learning attackers' tactics, techniques, and procedures (TTPs), it can predict subsequent intentions and potential attack paths. This shifts system operations from an "event-driven" to a "threat-driven" paradigm, enabling proactive adjustments such as preemptive hardening of heterogeneous entities predicted to be targeted [45].
3. **Dynamic Policy Optimization:** This represents AI's most transformative application. Through reinforcement learning and similar algorithms, systems frame dynamic scheduling as a sequential decision problem within a continuous adversarial interaction. By iteratively engaging with the environment (encompassing both attacks and system states), AI agents autonomously learn optimal scheduling strategies under specific security and performance constraints, ultimately achieving the long-term maximization of security utility [46]. This approach fundamentally addresses the efficiency and adaptability limitations of early random or rule-based schedulers.

Thus, the "AI + Endogenous Security" fusion inherently marries data-driven intelligence with structure-driven security. It evolves the architecture from a statically "immune" system into an intelligent organism equipped with both a "nervous system" for perception and a "learning brain" for adaptation. This synergy enables not only sharper threat perception and a deeper understanding of adversarial dynamics but also the autonomous optimization of intrinsic defense mechanisms, securing a decisive advantage in dynamic, complex cyber adversarial engagements.

4.2.2. Architectural Adaptation for Emerging Scenarios

The vitality of the endogenous security architecture stems from its core principle: it is not a static "silver bullet", but a "meta-methodology" that can be tailored, adapted, and optimized for specific scenarios. Confronted with the divergent architectures, resources, and requirements of emerging fields like 6G, cloud-native computing, and IoT edge computing, endogenous security is evolving toward lightweight, scenario-specific implementations. This ensures its security benefits can be embedded into every critical layer of future digital infrastructure at an acceptable cost.

1. "On-Demand Endogenous security" for 6G Network Slicing

The defining features of 6G networks are its service-based architecture and highly dynamic network slicing [47]. Integration here necessitates a shift from "device-level defense" to "slice-level endogenous security services". This is realized in two ways: First, core DHR components (e.g., heterogeneous redundant executors) are packaged as orchestratable security function modules. These are instantiated and injected into slices on demand—based on the distinct security and performance KPIs of slices like URLLC and mMTC—enabling service-oriented, differentiated security provisioning. Second, the dynamic scheduling and arbitration mechanisms of endogenous security must coordinate deeply with the network slicing orchestrator to synchronize security states with network resource states [48]. This not only enables on-demand security but also integrates it as a native component of the 6G security system.

2. "Declarative Endogenous security" in Cloud-Native Environments

Within microservices-based, containerized environments managed by Kubernetes, the endogenous security architecture must adhere to the principles of "declarative APIs" and "immutable infrastructure". The adaptation path involves: encapsulating heteroge-

neous executors as independent containerized Pods and leveraging Kubernetes controllers (e.g., custom Operators) to automate their deployment, scaling, and fault recovery—thus transforming dynamic scheduling into standard orchestration. Concurrently, the arbiter can be designed as a sidecar or agent within the service mesh, transparently intercepting and comparing microservice traffic non-intrusively to enable distributed, collaborative arbitration. Through this approach, endogenous security is woven into the cloud-native fabric, achieving a true fusion of security and operations.

3. “Lightweight Endogenous security” for IoT Edge Computing

IoT edge nodes face severe resource constraints and massive scale. Here, the classic DHR model requires extreme lightweight adaptation [49]. Key adjustments include:

- **Redundancy:** Moving from multi-copy, full-time redundancy to collaborative redundancy based on opportunistic communication or neighboring nodes—scheduling multiple adjacent nodes across time and space to jointly execute security-sensitive tasks [50].
- **Heterogeneity:** Shifting from deep hardware/OS diversity to lightweight differentiation via software configuration, algorithmic parameters, or compilation options.
- **Arbitration:** Adopting lightweight consensus algorithms or threshold-based local decisions to drastically reduce communication and computational overhead.

The goal is to enable edge devices to attain the core benefits of endogenous security while operating within strict cost and power limits.

The broad adaptability of the endogenous security architecture demonstrates that it is not a rigid blueprint, but a powerful “security design pattern”. Through service-oriented integration for 6G, cloud-native embedding, and edge-optimized lightweight solutions, it flexibly reshapes itself to become a universal methodology for building a comprehensive, end-to-end trusted foundation for the future digital world.

5. Application Evaluation and Challenges Outlook

5.1. Typical Application Domains and Performance Evaluation

The endogenous security paradigm has advanced from theoretical validation to a pivotal stage of large-scale industrial deployment. Its deep integration into two critical domains of information infrastructure—5G core networks and intelligent connected vehicles (ICV)—has not only proven its engineering feasibility but also yielded quantifiable security performance metrics, as detailed in Table 3.

Table 3. Performance Comparison of Typical Endogenous Security Application Cases.

Evaluation Dimension	5G Core Network Endogenous Security Micro-Segmentation	Endogenous Security DHR Architecture for Intelligent Connected Vehicles (ICVs)
Core Security Challenge	East–west lateral movement attacks within the cloud-based core network create a “single breach, network-wide compromise” risk.	The deep integration of functional safety and cybersecurity presents novel challenges for unified security assurance.
Deployment Architecture	A hybrid architecture combining centralized management with distributed data-plane plugins. Plugins are embedded within 5G virtualized network functions (VNFs/CNFs), while a central manager handles policy orchestration and situational awareness, enabling fine-grained isolation within resource pools.	Introduces a Dynamic Heterogeneous Redundancy (DHR) structure into the vehicle E/E architecture. This enables integrated defense via multiple heterogeneous execution entities, a multi-mode arbiter, and dynamic scheduling.

Table 3. Cont.

Evaluation Dimension	5G Core Network Endogenous Security Micro-Segmentation	Endogenous Security DHR Architecture for Intelligent Connected Vehicles (ICVs)
Measured Security Gains	1. Lateral Attack Blocking Rate: Effectively monitors and blocks internal lateral movement attacks [51]. 2. Service Availability: Maintains 99.999% reliability with negligible impact on service performance [52]. 3. Resource Overhead: CPU/Memory utilization does not exceed 3% of the host network function virtual machine [51].	1. Attack Success Rate Suppression: White-box testing shows the DHR architecture achieves 100% differential-mode suppression against uncertainty-based perturbations [20]. 2. Defense Coverage: Effectively counters both known and unknown threats without prior knowledge, spanning the pre-incident, during-incident, and post-incident lifecycle [16,20].
Application Maturity	Has passed centralized procurement testing and entered large-scale commercial deployment, currently securing approximately 200,000 network function virtual machines [51].	Has undergone extensive white-box testing and real-vehicle validation, and is now in the standardization and industrial implementation phase [16].

Table 3 Notes: Ref. [51] Performance data are derived from the pilot test report and technical white paper of China Mobile’s 5G core network endogenous security micro-segmentation system. Ref. [52] The high-availability metric (99.999%) is supported by performance evaluations of analogous protection mechanisms reported in related research (e.g., DSN 2024 proceedings). Refs. [16,20] The test results for the intelligent connected vehicle case are sourced from peer-reviewed publications in Security and Safety and IEEE Vehicular Technology Magazine, which provide comprehensive data from controlled white-box tests and field trials.

5.1.1. Case Study 1: Endogenous Security Micro-Segmentation in 5G Core Networks

This system tackles the “blind spots” of lateral attack threats in east–west traffic between internal elements of cloud-based core networks. By adopting a collaborative architecture that combines “centralized management plane control with data plane plug-in integration”, it embeds endogenous security mechanisms while maintaining carrier-grade performance, including 99.999% reliability and microsecond-level latency. Field tests show that the system effectively contains internal attack propagation with less than 3% resource overhead, resolving the traditional security-performance trade-off. The solution has achieved international standardization (GSMA FS.61 [36]) and large-scale commercial deployment, marking the evolution of endogenous security from a prototype concept to mainstream infrastructure.

5.1.2. Case Study 2: DHR Architecture for Endogenous Security in Intelligent Connected Vehicles

To address the converging demands of automotive functional safety and cybersecurity, this architecture integrates the DHR (Dynamic Heterogeneous Redundancy) model into vehicle E/E (electronic/electrical) architectures. By establishing heterogeneous redundant execution units coupled with a dynamic arbitration mechanism, it offers a unified methodology for mitigating inherent uncertainties, encompassing both random failures and malicious attacks. White-box testing has confirmed its 100% differential-mode suppression capability against unknown perturbations, thereby providing security assurance at the principle level for high-criticality scenarios such as autonomous driving.

5.1.3. Comparative Analysis and Paradigm Validation

The two cases presented above, spanning from the cloud to the edge, collectively validate the broad universality and robust engineering adaptability of the endogenous security paradigm.

The 5G core network case demonstrates the feasibility of implementing endogenous security within hyperscale, high-performance virtualized environments. The primary engineering challenge here resides in satisfying extreme constraints on performance and reliability. The innovative “lightweight data plane plug-in + centralized intelligent management” solution addresses this by decoupling security logic from the forwarding plane. This enables the integration of security capabilities with “zero-impact” on system performance, providing a valuable blueprint for analogous scenarios such as cloud data centers.

The intelligent connected vehicle case prospectively validates the applicability of endogenous security to resource-constrained, real-time, safety-critical embedded systems. Its core challenge lies in achieving effective redundant execution within the confines of limited automotive-grade computing resources while simultaneously meeting the stringent determinism requirements of functional safety standards (e.g., ISO 26262 ASIL-D [53]). The adopted solution involves a deep optimization of the DHR model (e.g., employing dual-model redundancy) and the architectural integration of endogenous security adjudication with traditional functional safety monitoring mechanisms. This approach achieves a genuine fusion of “security integration”, thereby paving new pathways for other critical embedded systems, including industrial control applications.

In summary, these two successful implementations demonstrate that endogenous security is not merely an abstract concept but a systematic engineering methodology. It is capable of tailoring architectures to precise domain-specific constraints—be they performance, resource availability, or security levels—while delivering quantifiable security enhancements. Together, they point to the next critical evolutionary step for endogenous security: a transition from successful but isolated system-level applications toward building holistic, cross-domain collaborative resilience. This transition represents an inevitable and essential direction for constructing the future “grand security” framework of cyberspace.

5.2. Feasibility and Cost–Benefit Trade-Offs

The endogenous security paradigm, exemplified by the Dynamic Heterogeneous Redundancy (DHR) model, achieves security gains through structural redundancy at the cost of additional resources and operational overhead. This section analyzes the primary cost components and proposes a multidimensional framework for evaluating its feasibility in industrial deployment.

5.2.1. Analysis of Resource and Operational Overhead

The overhead primarily comprises direct resource consumption and indirect management overhead. Direct costs arise from the additional computational resources (CPU and memory) required to maintain N-fold redundant execution entities. Studies show that through lightweight virtualization and intelligent scheduling, the actual steady-state resource overhead can be kept significantly below a linear increase—remaining under 3% in critical scenarios such as 5G core networks [51]. Indirect costs relate to increased operational complexity, including the construction and maintenance of heterogeneous resource pools, the configuration and tuning of dynamic policies, and fault diagnosis across diverse components.

The term “resource overhead” here refers specifically to the direct computational resources consumed by the operation of endogenous security mechanisms—such as dynamic redundant executors and arbiters—primarily measured as incremental CPU and memory usage. This metric is typically obtained by comparing the resource utilization of the host environment (e.g., network function virtual machines) with and without the security mechanisms enabled, under standard or steady-state workload conditions. For example, the “below 3%” reported in [51] belongs to this category. It should be noted that

this figure does not encompass the indirect management efforts or operational complexity involved in building heterogeneous resource pools and implementing dynamic scheduling.

5.2.2. A Multidimensional Cost–Benefit Trade-Off Framework

Deploying endogenous security is a risk-based engineering decision. Its feasibility depends on a multidimensional trade-off specific to the context:

Asset Criticality: The paradigm is most justified for protecting high-value core assets (e.g., critical infrastructure control systems), where the potential loss from a security breach far outweighs the defensive investment.

Threat Landscape Alignment: Its structural advantages offer maximum cost-effectiveness against advanced persistent threats (APTs), unknown vulnerabilities, and supply chain attacks—precisely the challenges that often elude conventional defenses.

Total Cost of Ownership Perspective: Evaluation must consider the lifecycle view, accounting for how its preventative nature reduces long-term operational security costs, business disruption losses, and reputational risk, not merely the initial investment.

In conclusion, the feasibility of endogenous security does not imply zero cost. It lies in the continuous optimization of technology and architecture to contain resource expenditure within acceptable bounds for target scenarios, thereby achieving structural security gains against unknown threats that are difficult to attain with traditional architectures. This represents a practical engineering path for managing advanced risks at a controlled cost.

5.3. Challenges Faced

The endogenous security paradigm has made significant strides in transitioning from innovative concept to large-scale industrial practice. Yet, its future as a foundational security paradigm for cyberspace hinges on overcoming persistent challenges across three critical dimensions: theory, engineering, and ecosystem [54].

5.3.1. Theoretical Challenges: From “Engineering Effectiveness” to “Rigorous Proof”

The mathematical foundations of endogenous security require strengthening to achieve the leap from empirical validation to formal proof.

- **Proofs of Strict Security Upper Bounds:** Presently, the efficacy of endogenous security, particularly the Dynamic Heterogeneous Redundancy (DHR) model, is supported primarily by experimental and probabilistic evidence. This empirical foundation, however, does not render formal worst-case proofs theoretically unattainable; rather, it defines a critical, open research frontier. The central challenge is to rigorously establish the theoretical upper bound of security gain in DHR architectures under stringent adversarial models—where attackers may possess advantages such as unbounded resources or partial knowledge of scheduling strategies. Successfully addressing this challenge would not refute the paradigm’s validity but would ground its core tenet—“structure determines security”—within a more robust and universal mathematical axiomatic system. This advancement would elevate endogenous security from a powerful engineering paradigm to a formally verifiable theoretical discipline, thereby enhancing its academic rigor and providing a principled foundation for designing next-generation, high-assurance architectures.
- **Quantitative Trade-off Models:** The dynamic, heterogeneous, and redundant nature of the paradigm inherently introduces overhead. The absence of a universal, quantifiable model to optimize the “security-performance-overhead” trilemma impedes precise engineering trade-offs during deployment.

5.3.2. Engineering Challenges: From “Lab Prototypes” to “Large-Scale Systems”

Scaling endogenous security architectures to complex, distributed real-world environments presents formidable hurdles.

- **Heterogeneous Resource Management:** Constructing and maintaining effective heterogeneous resource pools across hardware, OS, software, and cloud vendors is complex and costly. Automation toolchains for deployment, configuration, and operations remain immature, leading to high management overhead.
- **The Arbitration Accuracy-Efficiency Trade-off:** The arbiter’s false positives and negatives directly impact system availability and security. Simple rules struggle with complex outputs (e.g., AI inferences), causing high false alarms, while sophisticated models introduce prohibitive latency and computational cost.
- **Complexity of Distributed Deployment at Scale:** Current implementations focus on bounded, closed systems. Scaling to mega-systems spanning multiple domains, clouds, and endpoints (e.g., nationwide IoT) introduces unprecedented challenges in global state awareness, distributed consensus, and cross-domain policy coordination.

5.3.3. Ecosystem Challenges: From “Technical Silos” to “Security Foundations”

Widespread adoption depends on the holistic evolution of the broader industrial ecosystem, which faces several key barriers:

- **Supply-Chain Collaboration and Standardization:** In integrated domains like automotive, coordinated design and standardized interfaces across chips, OS, and software are essential. Current fragmented standards often relegate endogenous security to an “add-on” or custom solution, preventing its integration as a default design principle.
- **Integration with Legacy Systems and Processes:** Enterprises operate vast traditional security infrastructures and workflows. Endogenous security must demonstrate interoperability—sharing intelligence and coordinating responses—to avoid creating new “security silos”. Moreover, its dynamic nature challenges static, compliance-based audit and risk assessment frameworks.
- **Paradigm Inertia in Industry and Education:** The incumbent security industry, educational frameworks, and certification regimes are deeply entrenched in the traditional “signature-based detection” paradigm. Promoting endogenous security requires overcoming path dependencies in technical standards, economic models, and user perceptions.
- **Establishing New Metrics and Trust Frameworks:** Unlike traditional security measured by vulnerabilities and detection rates, endogenous security provides probabilistic, structural gains aimed at making attacks “unlikely to succeed”. Developing scientifically rigorous metrics and trust frameworks to quantify this “unbreached” state is therefore a critical ecosystem challenge.

Therefore, the future of endogenous security hinges not merely on technological advances but equally on systematic progress in ecosystem development, standards harmonization, and cognitive alignment. Overcoming these broader challenges is essential for its evolution from a promising concept into a robust paradigm capable of underpinning future digital infrastructure.

5.4. Future Research Directions

To address these challenges, the endogenous security paradigm is evolving along three primary avenues: service-oriented transformation, convergence with frontier technologies, and foundational mechanism innovation. These directions represent a natural and necessary extension of current technological and research trends.

5.4.1. Paradigm Shift: Security-As-A-Service (SaaS)

With the proliferation of cloud-native and zero-trust architectures, it has become imperative to abstract, decouple, and package core endogenous security capabilities—such as dynamic heterogeneous redundancy (DHR) constructs and intelligent adjudication—into orchestratable security primitives deliverable via APIs or service meshes [55]. Future research should focus on: (a) defining and standardizing interfaces for these security capabilities to ensure interoperability; (b) developing intelligent cloud-native orchestrators capable of dynamically chaining security capabilities based on application SLAs, real-time load, and threat intelligence; and (c) investigating coordination and trust mechanisms for endogenous security services across multi-cloud and multi-domain environments [56]. This shift will transition security from a model of “purchasing equipment” to one of “consuming services”, significantly lowering adoption barriers and operational overhead.

However, delivering endogenous security capabilities as services within a shared cloud-native environment critically depends on the well-defined management of trust boundaries and the assurance of strict tenant isolation. Future research must explore how to leverage the intrinsic properties of endogenous security architectures to reinforce isolation guarantees in multi-tenant settings, alongside designing corresponding trusted measurement and verification mechanisms. Such exploration is essential to fully embrace the agility and cost benefits of the service-based model while preserving its core security attributes.

5.4.2. Technology Convergence: Deep Integration with Quantum-Safe Technologies

Quantum computing and endogenous security represent two pivotal pathways toward next-generation security. Their deep integration is crucial to mitigating fundamental threats like cryptographic breaches enabled by vast computational power. Key intersections include: (a) integrating post-quantum cryptography (PQC) algorithms as core heterogeneous components within execution entities to strengthen cryptographic foundations, while addressing associated challenges such as high computational overhead and integration complexity [57]; (b) exploring synergies between quantum communication technologies (e.g., quantum key distribution) and endogenous security architectures to provide new trust anchors for secure communications among arbitrators or execution entities; and (c) leveraging the endogenous security philosophy of managing “uncertainty” to inform the design of resilient post-quantum security protocols and agile migration frameworks [58].

5.4.3. Mechanism Innovation: Bio-Inspired Endogenous Defense

Moving beyond conventional engineering models, drawing inspiration from sophisticated defense mechanisms honed by natural evolution—such as immune systems and swarm intelligence—holds promise for foundational innovation [59]. Exploratory research may focus on: (a) emulating adaptive immunity and immune memory, enabling systems to dynamically generate specific countermeasures against novel attacks and scale down defenses post-threat efficiently; (b) designing distributed consensus-based immunity, inspired by the self-organizing behaviors of social insects or flocks, to create collaboration algorithms that achieve global threat containment and recovery through localized interactions without a central authority [60]; and (c) implementing wound-healing and regeneration analogs, allowing systems not only to isolate faults but also to autonomously reallocate resources and reconfigure functionalities for true survivability and evolutionary adaptation [61].

6. Conclusions

The endogenous security paradigm, as an original concept that reconceptualizes the traditional “add-on patching” model, has evolved through a coherent trajectory—from

philosophical inquiry and theoretical modeling to architectural implementation and industrial practice. This development originates from a profound insight into the intrinsic contradictions of cyberspace, is grounded in the core axiom of Dynamic Heterogeneous Redundancy (DHR), and was initially validated through early mimic defense prototypes. Driven by standardization and foundational technologies, the architecture has subsequently advanced: heterogeneity has expanded from the physical to the virtual and algorithmic layers, dynamic strategies have evolved from randomization to intelligence, and adjudication mechanisms have progressed from simple voting to behavioral analysis. This progression not only confirms the engineering feasibility of the “structure-determines-security” tenet but also yields quantifiable security gains in critical infrastructures such as 5G core networks and intelligent connected vehicles, solidifying its role as a paradigm innovator in cyberspace security.

Currently, endogenous security stands at a pivotal transition from a phase of innovative breakthroughs toward scalable maturity. This shift presents clear imperatives for both academia and industry. For researchers, the priority is to bridge the gap from empirical effectiveness to formal proofs of security and to deepen the exploration of its integration with frontier technologies such as artificial intelligence, cloud-native computing, and quantum-safe mechanisms. For practitioners, the focus must shift to tackling systemic engineering challenges, including the management of heterogeneous resources and large-scale distributed coordination, and to promoting the productization and service-orientation of core capabilities (e.g., DHR constructs) to lower adoption barriers. Ultimately, widespread deployment will depend on fostering a synergistic ecosystem that integrates industry, academia, research, and application—spanning the full technology stack from silicon and system software to applications—and ensuring alignment with existing security frameworks and international standards.

At its core, the endogenous security paradigm contributes a foundational direction for future network infrastructure: toward endogenous resilience and autonomous evolution. It reorients the design philosophy from a singular pursuit of performance and functionality toward the native co-evolution of security, functionality, and performance in open, adversarial environments. For instance, guided by this philosophy, a cloud data center architect would no longer begin by selecting the most advanced intrusion detection system. Instead, the design would be reconsidered from first principles: how to dynamically orchestrate heterogeneous instances from different virtualization platforms and container runtimes to host the same critical service, how to implement a lightweight behavioral arbiter for real-time output comparison, and how to orchestrate instance refresh and recovery based on threat intelligence. This exemplifies the shift in security from an “add-on component” to a “first principle” of architectural design. It marks a profound paradigm shift—cyberspace security is moving beyond exogenous “add-ons and patches” to become an endogenous property of “growth and immunity”, charting a course for its continuous evolution into more advanced and intrinsic forms.

Author Contributions: Conceptualization, H.Z. and J.L.; methodology, H.Z. and H.W. (Hong Wang); software, H.Z.; validation, H.Z., S.X. and H.Y.; formal analysis, J.L.; investigation, H.W. (Hong Wang); resources, H.Z.; data curation, S.X.; writing—original draft preparation, H.Z.; writing—review and editing, H.W. (Haitao Wu); visualization, S.X.; supervision, H.W. (Haitao Wu); project administration, H.Z.; funding acquisition, H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DHR Dynamic Heterogeneous Redundancy
APT Advanced Persistent Threat

References

1. Wu, J. Cyberspace Endogenous Safety and Security. *Engineering* **2022**, *15*, 179–185. [\[CrossRef\]](#)
2. Wu, J. *Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security*; Wireless Networks; Springer International Publishing: Cham, Switzerland, 2020.
3. Mahboubi, A.; Luong, K.; Aboutorab, H.; Bui, H.T.; Jarrad, G.; Bahutair, M.; Camtepe, S.; Pogrebna, G.; Ahmed, E.; Barry, B.; et al. Evolving Techniques in Cyber Threat Hunting: A Systematic Review. *J. Netw. Comput. Appl.* **2024**, *232*, 104004. [\[CrossRef\]](#)
4. Ma, M.; Zhu, T.; Li, S.; Chen, T.; Lv, M.; Weng, Z.; Chen, G. ActMiner: Applying Causality Tracking and Increment Aligning for Graph-Based Cyber Threat Hunting. *Knowl.-Based Syst.* **2025**, *327*, 114169. [\[CrossRef\]](#)
5. Wu, J. *Cyber Resilience System Engineering Empowered by Endogenous Security and Safety*; Springer Nature Singapore: Singapore, 2024.
6. Ji, X.; Wu, J.; Jin, L.; Huang, K.; Chen, Y.; Sun, X.; You, W.; Huo, S.; Yang, J. Discussion on a New Paradigm of Endogenous Security towards 6G Networks. *Front. Inf. Technol. Electron. Eng.* **2022**, *23*, 1421–1450. [\[CrossRef\]](#)
7. Shao, S.; Ji, Y.; Zhang, W.; Liu, S.; Jiang, F.; Cao, Z.; Wu, F.; Zeng, F.; Zuo, J.; Zhou, L. A DHR Executor Selection Algorithm Based on Historical Credibility and Dissimilarity Clustering. *Sci. China Inf. Sci.* **2023**, *66*, 212304. [\[CrossRef\]](#)
8. Wu, J. Problems and Solutions Regarding Generalized Functional Safety in Cyberspace. *Secur. Saf.* **2022**, *1*, 2022001. [\[CrossRef\]](#)
9. Brembilla, L. The Effect of the Social Security on Aggregate Effective Labor Supply: The Role of Endogenous Human Capital and of Selection Effects. *Macroecon. Dyn.* **2025**, *29*, e44. [\[CrossRef\]](#)
10. Liu, X.; Wang, H.; Li, C. A Review of Endogenous Security Research. *Electronics* **2024**, *13*, 2185. [\[CrossRef\]](#)
11. Sun, R.; Zhu, Y.; Fei, J.; Chen, X. A Survey on Moving Target Defense: Intelligently Affordable, Optimized and Self-Adaptive. *Appl. Sci.* **2023**, *13*, 5367. [\[CrossRef\]](#)
12. Wu, J. On the Revolution of the Information Network Development Paradigm. *Sci. China Inf. Sci.* **2022**, *65*, 213301. [\[CrossRef\]](#)
13. Huang, Z.; Yuan, Y.; Fu, J.; He, J.; Zhu, H.; Cheng, G. Location-Aware Measurement for Cyber Mimic Defense: You Cannot Improve What You Cannot Measure. *Appl. Sci.* **2023**, *13*, 9213. [\[CrossRef\]](#)
14. Shi, L.; Wang, B.; Li, A.; Zhang, H. Exploiting Self-Evolutionary Strategies of Components for Dynamic Heterogeneous Redundancy. *Comput. Electr. Eng.* **2024**, *120*, 109756. [\[CrossRef\]](#)
15. Wu, X.; Wang, M.; Shen, J.; Gong, Y. Towards Double-Layer Dynamic Heterogeneous Redundancy Architecture for Reliable Railway Passenger Service System. *Electronics* **2024**, *13*, 3592. [\[CrossRef\]](#)
16. Liu, Q.; Wang, Z.; Wang, P.; Li, Y.; Zheng, X.; Tang, P. Dynamic Heterogeneous Redundancy-Based Endogenous Security and Safety for Connected Automated Vehicles: Preliminary Test Results and Assessment. *Secur. Saf.* **2026**, *4*, 2025009. [\[CrossRef\]](#)
17. Kang, Y.; Zhang, Q.; Jiang, B.; Bu, Y. A Differentially Private Framework for the Dynamic Heterogeneous Redundant Architecture System in Cyberspace. *Electronics* **2024**, *13*, 1805. [\[CrossRef\]](#)
18. Chen, Z.; Cui, G.; Zhang, L.; Yang, X.; Li, H.; Zhao, Y.; Ma, C.; Sun, T. Optimal Strategy for Cyberspace Mimic Defense Based on Game Theory. *IEEE Access* **2021**, *9*, 68376–68386. [\[CrossRef\]](#)
19. Dai, W.; Li, S.; Lu, L.; Ye, Y.; Meng, F.; Zhang, D. Research on Application of Mimic Defense in Industrial Control System Security. In Proceedings of the 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 17–19 December 2021; Volume 2, pp. 573–577.
20. Li, Y.; Liu, Q.; Zhuang, W.; Zhou, Y.; Cao, C.; Wu, J. Dynamic Heterogeneous Redundancy-Based Joint Safety and Security for Connected Automated Vehicles: Preliminary Simulation and Field Test Results. *IEEE Veh. Technol. Mag.* **2023**, *18*, 89–97. [\[CrossRef\]](#)
21. Chen, P.; Wei, J.; Yu, Z.; Chen, J. Key-Area Cyberspace Mimic Defense against Data-Oriented Attacks. *Secur. Saf.* **2025**, *4*, 2024015. [\[CrossRef\]](#)
22. Wu, J.; Zou, H.; Chen, J.; Zhang, F.; Shang, Y.; Ji, X. On Cultivation of Cybersecurity and Safety Talents and Responsible Developers. *Secur. Saf.* **2024**, *3*, 2024010. [\[CrossRef\]](#)
23. Jin, L.; Hu, X.; Wu, J. From Perfect Secrecy to Perfect Safety & Security: Cryptography-Based Analysis of Endogenous Security. *Secur. Saf.* **2023**, *2*, 4–19.

24. Guan, L.; Tao, C.; Chen, P. Research on Endogenous Security Defense for Cloud-Edge Collaborative Industrial Control Systems Based on Luenberger Observer. *Mathematics* **2025**, *13*, 2703. [\[CrossRef\]](#)
25. Li, Z.; Hu, Y.; Wu, J.; Lu, J. P4Resilience: Scalable Resilience for Multi-Failure Recovery in SDN with Programmable Data Plane. *Comput. Netw.* **2022**, *208*, 108896. [\[CrossRef\]](#)
26. Wu, J. Development Paradigms of Cyberspace Endogenous Safety and Security. *Sci. China Inf. Sci.* **2022**, *65*, 156301. [\[CrossRef\]](#)
27. Xu, C.; Wu, J.; Zhang, F.; Freer, J.; Zhang, Z.; Cheng, Y. A Deep Image Classification Model Based on Prior Feature Knowledge Embedding and Application in Medical Diagnosis. *Sci. Rep.* **2024**, *14*, 13244. [\[CrossRef\]](#)
28. Xu, M.; Guo, J.; Yuan, H.; Yang, X. Zero-Trust Security Authentication Based on SPA and Endogenous Security Architecture. *Electronics* **2023**, *12*, 782. [\[CrossRef\]](#)
29. Ren, Q.; Hu, T.; Wu, J.; Hu, Y.; He, L.; Lan, J. Multipath Resilient Routing for Endogenous Secure Software Defined Networks. *Comput. Netw.* **2021**, *194*, 108134. [\[CrossRef\]](#)
30. Zhu, Z.; Yu, H.; Liu, Q.; Liu, D.; Yu, H. An Adaptive Multiexecutors Scheduling Algorithm Based on Heterogeneity for Cyberspace Mimic Defense. *Secur. Commun. Netw.* **2022**, *2022*, 2300407. [\[CrossRef\]](#)
31. Luo, M.; Tao, C.; Liu, Y.; Chen, S.; Chen, P. An Endogenous Security-Oriented Framework for Cyber Resilience Assessment in Critical Infrastructures. *Appl. Sci.* **2025**, *15*, 8342. [\[CrossRef\]](#)
32. Yu, X.; He, L.; Geng, J.; Liang, Z.; Gan, Z.; Zhao, H. Dynamic Defense Strategy Selection Through Reinforcement Learning in Heterogeneous Redundancy Systems for Critical Data Protection. *Appl. Sci.* **2025**, *15*, 9111. [\[CrossRef\]](#)
33. T/ZGTXHX 043—2022; Network 5.0 Intrinsic Security Architecture. China Institute of Communications: Beijing, China, 2022.
34. T/NJCESS 003—2024; Technical specification of endogenous security network controller. Nanjing Cyberspace Endogenous Security Association: Nanjing, China, 2024.
35. Zhang, C.; Zhang, T.; Zhao, Y. SemanticICV: Endogenous Secure Full-Scenario Learning for Intelligent Connected Vehicles Driven by Semantics. *IEEE Netw. Mag. Comput. Commun.* **2024**, *38*, 156–163. [\[CrossRef\]](#)
36. GSMA FS.61; Micro-Segmentation in 5G Core Network Resource Pool Guidelines: Version 1.0. GSMA: London, UK, 2025.
37. Ogbodo, E.U.; Abu-Mahfouz, A.M.; Kurien, A.M. A Survey on 5G and LPWAN-IoT for Improved Smart Cities and Remote Area Applications: From the Aspect of Architecture and Security. *Sensors* **2022**, *22*, 6313. [\[CrossRef\]](#)
38. YD/T 6021—2024; Technical Requirements for Cloudified Telecommunications Network Micro-segmentation System. China Communications Standards Association: Beijing, China, 2024.
39. Xi, W.; Li, X.; Feng, Q.; Yao, H.; Cai, T.; Yu, Y. Cyber Security Protection of Power System Equipment Based on Chip-Level Trusted Computing. *Front. Energy Res.* **2022**, *10*, 842938. [\[CrossRef\]](#)
40. Liu, D.; Wang, S.; Shi, C.; Li, J.; Jiang, X. Application and Optimization of Endogenous Security Mechanisms in Photovoltaic Data Transmission and Storage. *Appl. Math. Nonlinear Sci.* **2025**, *10*, 20250223. [\[CrossRef\]](#)
41. Ma, Y.; Yu, C.; Weng, C. Morpheus: An Efficient Timing-Based Attestation Framework for Safeguarding Hypervisor Integrity with Dynamic Trust. *Comput. Secur.* **2024**, *144*, 103966. [\[CrossRef\]](#)
42. Farooq, M.S.; Riaz, S.; Alvi, A. Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review. *Electronics* **2023**, *12*, 3077. [\[CrossRef\]](#)
43. Fernandez, E.B.; Muñoz, A. A Cluster of Patterns for Trusted Computing. *Int. J. Inf. Secur.* **2025**, *24*, 72. [\[CrossRef\]](#)
44. Zhang, F.; Chen, X.; Huang, W.; Wu, J.; Zhang, Z.; Zhou, C.; Li, J.; Peng, Z.; Guo, W.; Yang, G.; et al. Harnessing Dynamic Heterogeneous Redundancy to Empower Deep Learning Safety and Security. *Secur. Saf.* **2024**, *3*, 2024011. [\[CrossRef\]](#)
45. Mitropoulou, K.; Kokkinos, P.; Soumplis, P.; Varvarigos, E. Anomaly Detection in Cloud Computing Using Knowledge Graph Embedding and Machine Learning Mechanisms. *J. Grid Comput.* **2024**, *22*, 6. [\[CrossRef\]](#)
46. Gao, B.; Chen, L.; Lin, L.; Huang, Y. Endogenous Security-Based Load Balancing Secure Routing for UAVs with Three-Layer Architecture. *J. Chin. Inst. Eng.* **2025**, *48*, 792–803. [\[CrossRef\]](#)
47. Lv, J. Research on the Legal Liability Distribution Mechanism of Cybersecurity under the Endogenous Security Concept of 6G Networks. *Acad. J. Humanit. Soc. Sci.* **2024**, *7*, 92–97. [\[CrossRef\]](#)
48. Kummerow, A.; Abrha, E.; Eisenbach, M.; Rösch, D. Unsupervised Anomaly Detection and Explanation in Network Traffic with Transformers. *Electronics* **2024**, *13*, 4570. [\[CrossRef\]](#)
49. Aledhari, M.; Razzak, R.; Rahouti, M.; Yazdinejad, A.; Parizi, R.M.; Qolomany, B.; Guizani, M.; Qadir, J.; Al-Fuqaha, A. Safeguarding Connected Autonomous Vehicle Communication: Protocols, Intra- and Inter-Vehicular Attacks and Defenses. *Comput. Secur.* **2025**, *151*, 104352. [\[CrossRef\]](#)
50. Nguyen, M.; Debroy, S. Moving Target Defense-Based Denial-of-Service Mitigation in Cloud Environments: A Survey. *Secur. Commun. Netw.* **2022**, *2022*, 2223050. [\[CrossRef\]](#)
51. Dixit, U.; Vittal, S.; A, A.F. A Systematic Study for Understanding the Security Risks in 5G Core Network. In Proceedings of the 2024 16th International Conference on Communication Systems & NETWORKS (COMSNETS), Bengaluru, India, 3–7 January 2024; pp. 43–48.

52. Maitra, S.; Atalay, T.O.; Stavrou, A.; Wang, H. Towards Shielding 5G Control Plane Functions. In Proceedings of the 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Brisbane, QLD, Australia, 24–27 June 2024; pp. 302–315.
53. ISO 26262:2018; Road vehicles — Functional safety. International Organization for Standardization: Geneva, Switzerland, 2018.
54. Wu, J.; Zou, H.; Xue, X.; Zhang, F.; Shang, Y. Cyber Resilience Enabled by Endogenous Security and Safety: Vision, Techniques, and Strategies. *Strateg. Study CAE* **2023**, *25*, 106. [\[CrossRef\]](#)
55. Meng, W.; Li, W.; Zhou, J. Enhancing the Security of Blockchain-Based Software Defined Networking through Trust-Based Traffic Fusion and Filtration. *Inf. Fusion* **2021**, *70*, 60–71. [\[CrossRef\]](#)
56. Park, H.; El Azzaoui, A.; Park, J.H. AIDS-Based Cyber Threat Detection Framework for Secure Cloud-Native Microservices. *Electronics* **2025**, *14*, 229. [\[CrossRef\]](#)
57. Saki, A.A.; Alam, M.; Phalak, K.; Suresh, A.; Topaloglu, R.O.; Ghosh, S. A Survey and Tutorial on Security and Resilience of Quantum Computing. *arXiv* **2021**, arXiv:2106.06081. [\[CrossRef\]](#)
58. Thangamani, R.; Vimaladevi, M.; Kamalam, G.K.; Subramanian, K.M. Securing the Future: Quantum Computing in Cybersecurity. In *Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategies*; Goyal, S.B., Kumar, V., Islam, S.M.N., Ghai, D., Eds.; Springer Nature: Singapore, 2025; pp. 441–487.
59. Anderson, W.; Moore, K.; Ables, J.; Mittal, S.; Rahimi, S.; Banicescu, I.; Seale, M. Designing an Artificial Immune System Inspired Intrusion Detection System. *arXiv* **2022**, arXiv:2208.07801. [\[CrossRef\]](#)
60. Chui, K.T.; Liu, R.W.; Zhao, M.; Zhang, X. Bio-Inspired Algorithms for Cybersecurity—A Review of the State-of-the-Art and Challenges. *Int. J. Bio-Inspired Comput.* **2024**, *23*, 1–15. [\[CrossRef\]](#)
61. Sharma, R.K.; Issac, B.; Xin, Q.; Gadekallu, T.R.; Nath, K. Plant and Salamander Inspired Network Attack Detection and Data Recovery Model. *Sensors* **2023**, *23*, 5562. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.